



# Instructions for Establishing a Free Email Account

## *NC DHHS BEACON HR/Payroll System Implementation*

*Date Created: February 5, 2008*

*Date Updated: February 6, 2008*

*Version: 19*

### **Introduction**

All DHHS employees require an email address to obtain an NC Identity (NCID) account, which in turn all DHHS employees need to access the State's BEACON HR/Payroll System. This document is intended for use by all DHHS employees who have neither a State-provided nor a personal email account established and provides instructions on how to establish an email account using common providers of free email services.

**Note.** DIRM selected the list of providers included herein based on popularity. NC DHHS neither endorses nor limits State employees from using any specific free email provider.

### **General Conditions**

- Employees must adhere to the Acceptable Use for DHHS Information Systems Policy (refer to ***Appendix E: Acceptable Use for DHHS Information Systems***).
- Each employee is responsible for managing his or her own user name, password, storage limits, and account expiration.
- DIRM's IT Customer Support Unit will provide limited guidance to employees seeking assistance. Specifically, agents in the IT Customer Support Unit will point employees to the appropriate online help or telephone number provided by the free email provider.
- Employees without computer access shall seek assistance from division/office HR or IT personnel to access PCs in training

rooms and/or other available PC resources until kiosks (i.e., communal/shared PCs) are available.

- The allowance to use a free email account to obtain an NCID is restricted to employees who do not have a State-provided email account.

### General Instructions

1. Select one free email provider from the following list:
  - Yahoo Mail
  - Google Mail (a.k.a., G-mail)
  - Microsoft Hotmail
  - America Online (a.k.a., AOL)
2. Follow the step-by-step instructions provided in the Appendix that corresponds to the free email provider selected in step 1

For this free email provider...	...refer to this Appendix for instructions
Yahoo Mail	Appendix A
Google Mail (a.k.a., G-mail)	Appendix B
Microsoft Hotmail	Appendix C
America Online (a.k.a., AOL)	Appendix D

3. Inform your NCID Administrator that you have established an email account and are ready to establish an NCID account

**Appendix A: How to Create a Yahoo Mail Email account**

Yahoo Mail is an online email service by Yahoo, and gives the user up to 2 GB of storage as of January 2008.

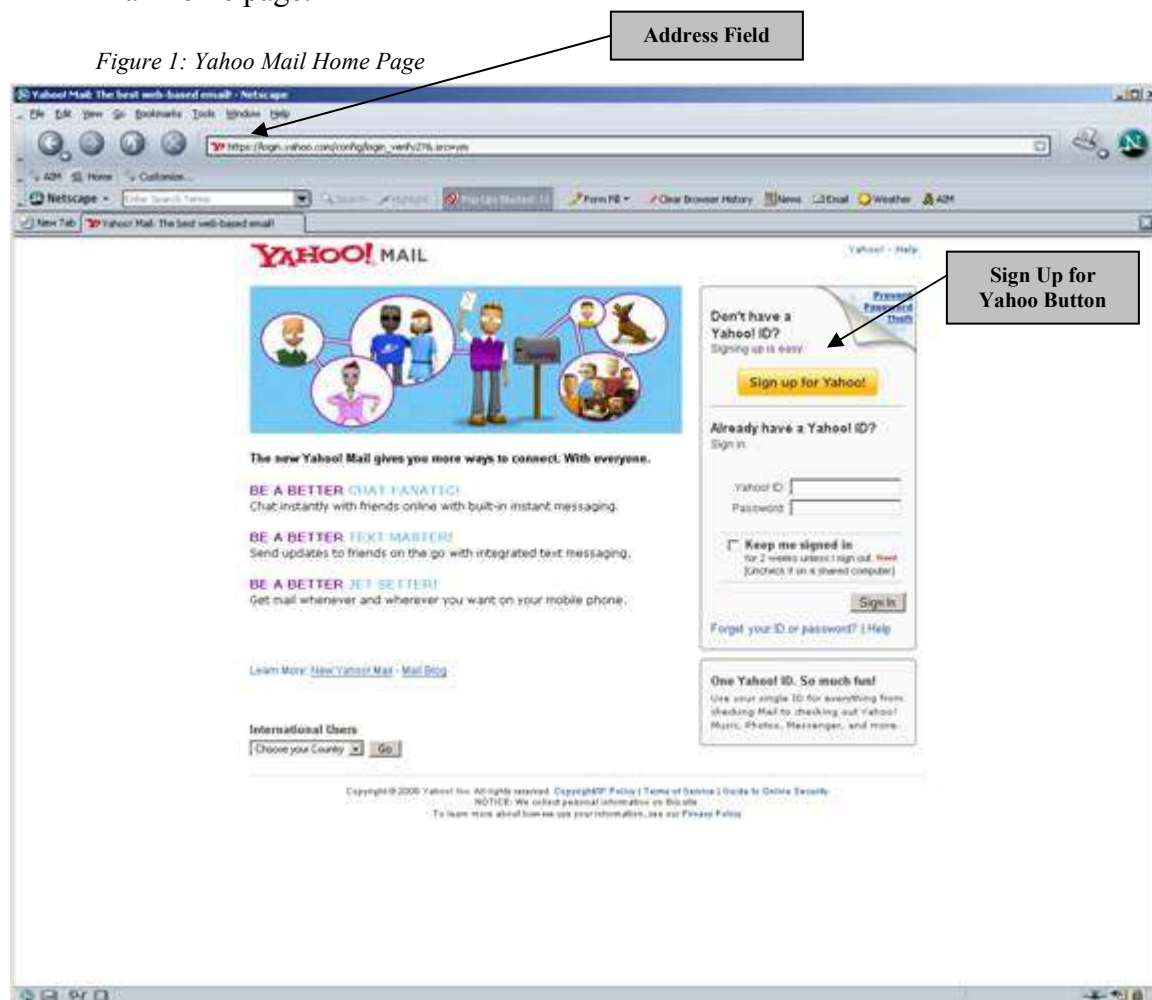
Here is how to create your free Yahoo Mail account:

1. Open your preferred web browser (e.g., Internet Explorer, Netscape Navigator, Mozilla Firefox, and Apple Safari).

The home page for your web browser will appear.

2. In the Address field, type <http://mail.yahoo.com> and press the Enter or Return key on your keyboard. This opens the Yahoo Mail home page.

Figure 1: Yahoo Mail Home Page



3. Click the yellow 'Sign up for Yahoo' button on the upper right side of the web page as shown in Figure 1. This opens the Yahoo Sign up page as depicted in Figure 2

Figure 2: Yahoo Sign up Page

The screenshot shows the Yahoo! Registration page in a Netscape browser window. The page has a light gray background with the Yahoo! logo at the top left. A cartoon character says "Hi there!" and explains that the user will be set up in three easy steps. There are links for "Already have an ID or Mail address?" (Sign In) and "Forgot your password or Yahoo! ID?". A dropdown menu shows "I prefer content from Yahoo! U.S. in English".

**1. Tell us about yourself...**

My Name: [Text Field]  
Gender: [Select One]  
Birthday: [Select Month] [Text Field]  
I live in: [United States]  
Postal Code: [Text Field]

**2. Select an ID and password**

Yahoo! ID and Email: [Text Field] @ yahoo.com  
Password: [Text Field]  
Re-type Password: [Text Field]

**3. In case you forget your ID or password...**

Alternate Email: [Text Field]  
Security Question: [Select One]  
Your Answer: [Text Field]

**Just a couple more details...**

Type the code shown: [Text Field] 7G84T

Do you agree? ☐ I have read and agree to the Yahoo! Terms of Service and Yahoo! Privacy Policy, and to receive important communications from Yahoo! electronically.  
For your convenience, these documents will be emailed to your Yahoo! Mail account.

[Create My Account](#) [Cancel](#)

Figure 3 illustrates a close up of the fields you will fill in for your account creation. Several of these fields are mandatory.

Figure 3: Close-up of Account Creation Fields

**1. Tell us about yourself...**

My Name

Gender

Birthday

I live in

Postal Code

**2. Select an ID and password**

Yahoo! ID and Email  @ yahoo.com

Password

Re-type Password

**3. In case you forget your ID or password...**

Alternate Email

Security Question

Your Answer

---

Just a couple more details...

Type the code shown

7G8zLT

Do you agree? ☐ I have read and agree to the [Yahoo! Terms of Service](#) and [Yahoo! Privacy Policy](#), and to receive important communications from Yahoo! electronically.  
For your convenience, these documents will be emailed to your Yahoo! Mail account.

5. Enter your first name, then last name in the **My Name** fields.
6. Select the appropriate gender from the drop down **Gender** menu.
7. Select your birth month from the drop down menu to the right of **Birthday**, then type in your birth day in the next field and your birth year in the third field on the line.
8. Keep the default selected in the '**I live in**' field set to United Sates
9. Type your five-digit work zip code in the Postal Code field.  
For example, Dix campus employees would insert 27603.

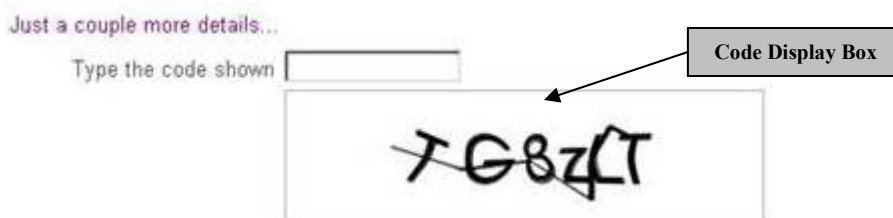
10. Select an ID, which will become your Yahoo Email address. Examples of a Yahoo ID and Email Address are:

- John.smith
- Jane\_Doe
- John1234

Click the '**Check**' button, after typing an ID into the '**Yahoo ID and Email**' field, to see if it is available.

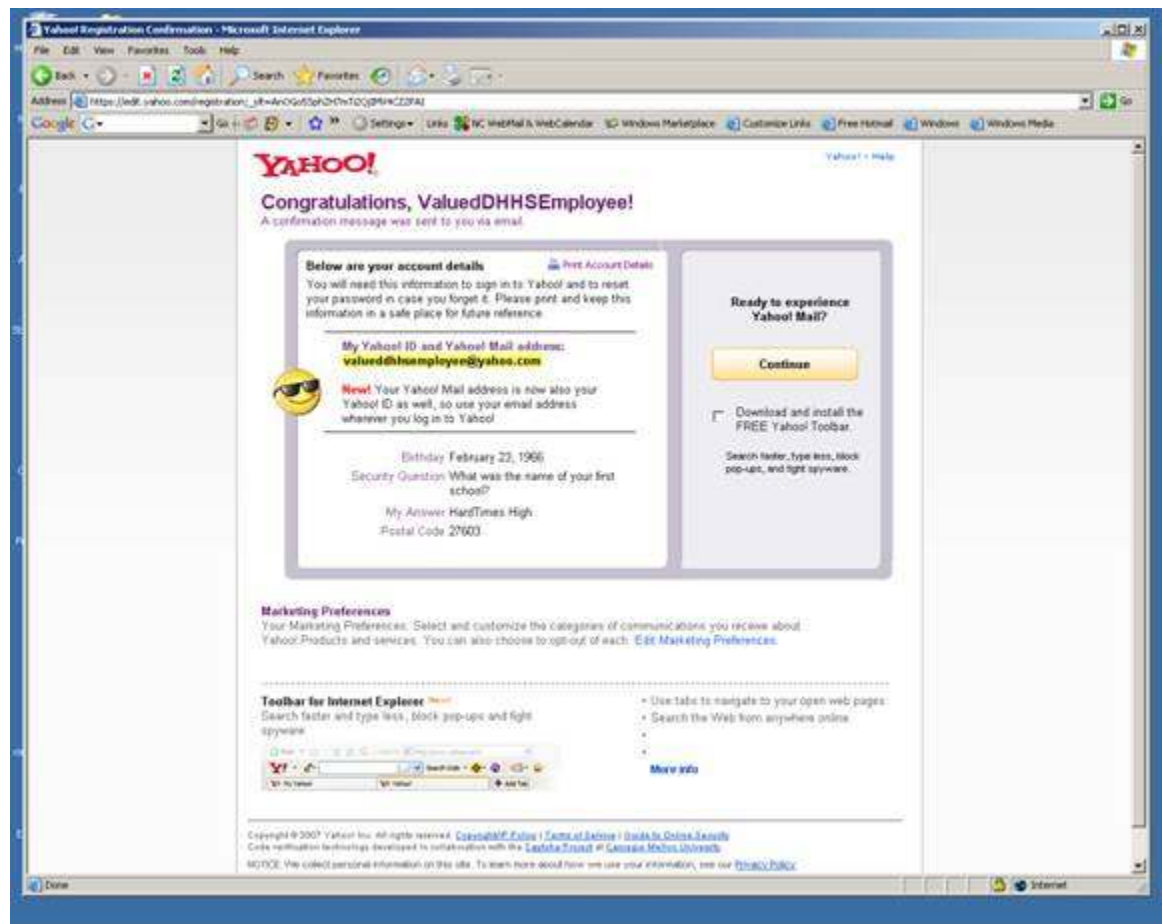
11. Once validated, go to the **Password** field, and enter the desired password. The desired password should be at least seven characters in length, using both letters and numbers. Re-enter your desired password in the **Retype password** field.
12. Skip the **Alternate Email** field, unless otherwise needed.
13. Click in the drop down menu next to the **Security Question** field and select a security question. Provide an answer in the **Your Answer** field.
14. Enter the displayed code in the **Type the code shown** field as seen in the code display box. The code is not case sensitive and may include upper and lower case characters.

Figure 4: Code Display Box



15. Optionally, review the Yahoo Terms of Service or the Yahoo Privacy Policy Agreement(s), by clicking on the provided links. After review, as desired, click the box to the right of **Do you agree?**
16. Finally, click on the 'Create My Account' button. Presented is a page similar to that depicted in Figure 5 and you have completed the registration process for your free Yahoo email account.

Figure 5: Yahoo Mail Account Creation Congratulations Page



## Appendix B: How to Create a Google Gmail Email Account

Gmail is an online email service by Google, and its main attractions are no banner advertisements and the huge amount of storage space for email they give you: 3407 MB as of October 2007.

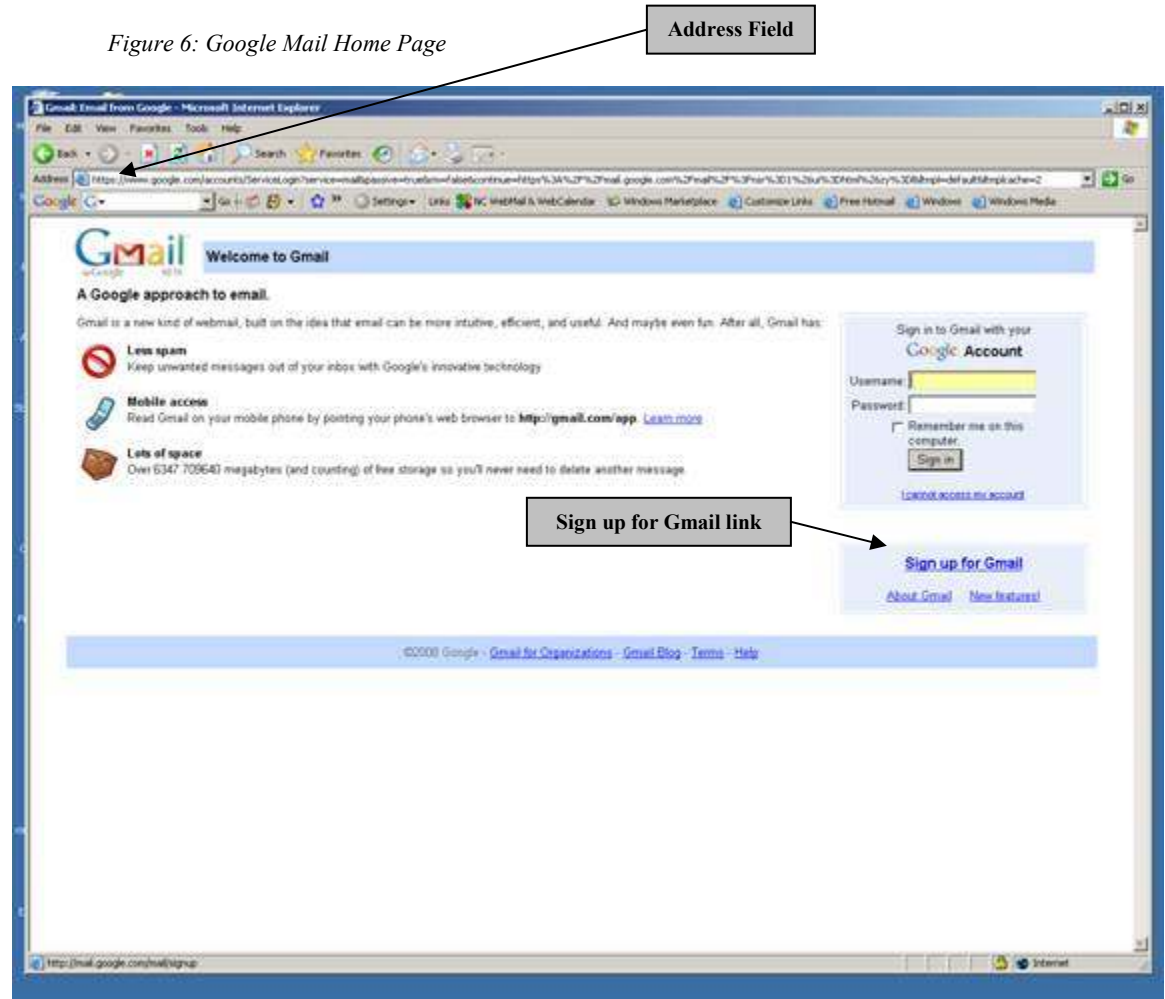
Here is how to create your free Gmail account:

1. Open your preferred web browser (e.g., Internet Explorer, Netscape Navigator, Mozilla Firefox, and Apple Safari).

The home page for your web browser will appear.

2. In the **Address** field, type <http://mail.google.com> and press the Enter or Return key on your keyboard. This will take you to the Google Gmail home page as seen in Figure 6 below.

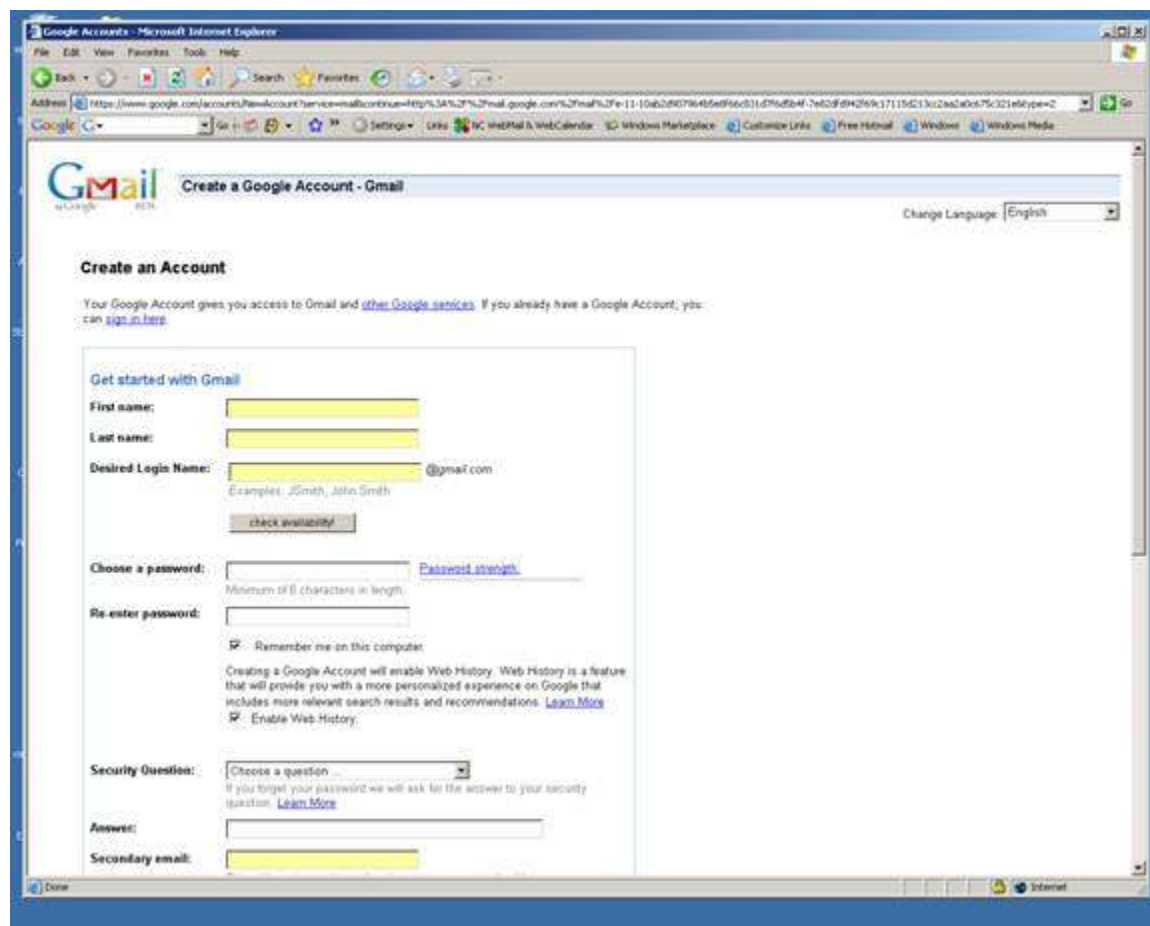
Figure 6: Google Mail Home Page



3. Click the 'Sign up for Gmail' link, identified in Figure 6 above. This takes you to the 'Create an Account' screen as depicted in Figure 7.



Figure 7: Google Mail Create an Account Page



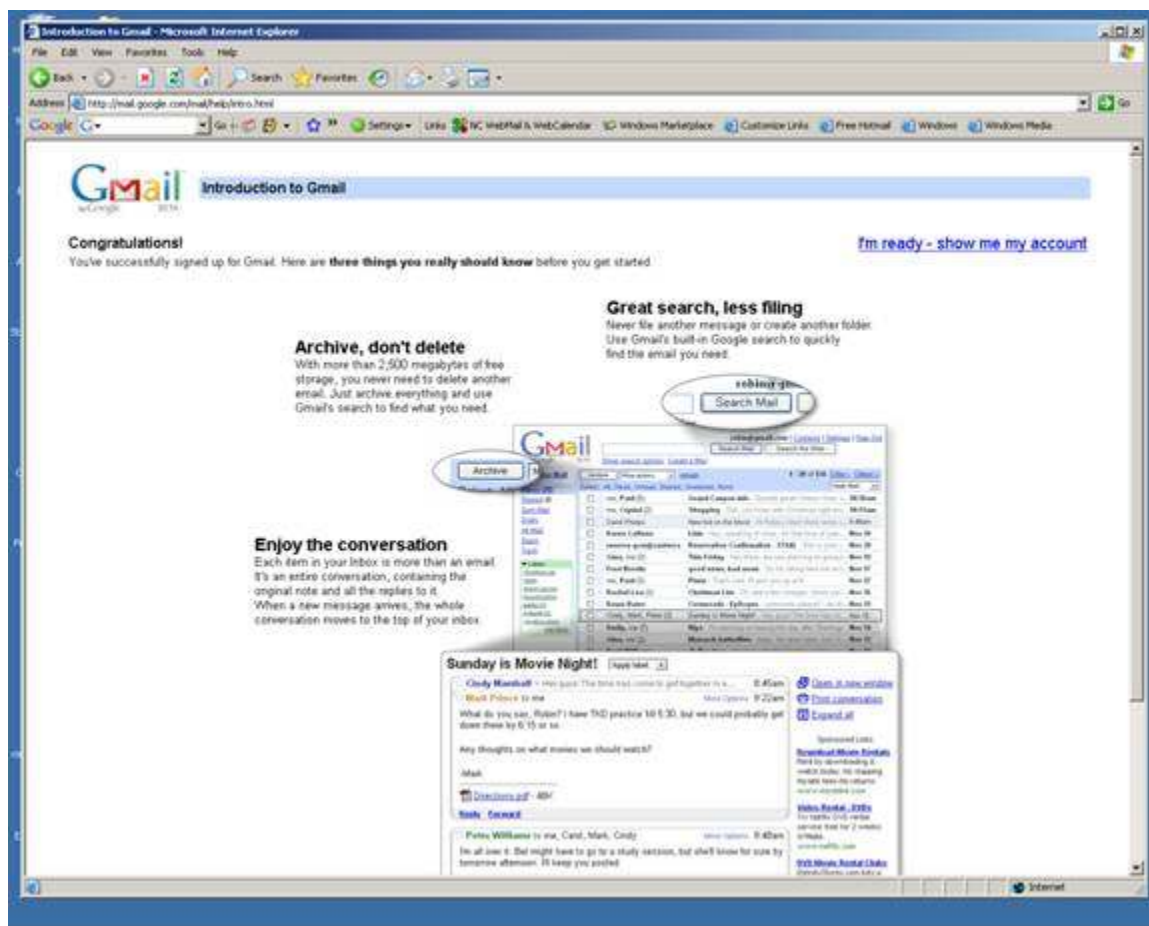
There are several mandatory fields in the window you will now fill including First Name, Last Name and Desired Login Name.

4. Enter your First Name and Last Name in the appropriate fields.
5. Enter the desired login name in the **Desired Login Name** field. Examples of a desired login name are:
  - John.smith
  - Jane\_Doe
  - John1234
6. Once entered, click the 'Check Availability!' button to see if the desired name is available for use. If not, try another name and repeat. This will be your unique Gmail email address.
7. After selecting a valid desired login name, go to the **Choose a password** field and enter the desired password. The password must be at least eight characters in length. Re-enter your

desired password in the **Re-enter password** field. Uncheck the 'Remember me on this computer' and 'Enable Web History' fields.

8. Next, select a security question from the drop down menu next to **Security Question**. Once selected, provide an answer to the question in the **Answer** field. The **Secondary email** field is available if desired.
9. Keep the default setting for the **Location** field set to United States.
10. Enter the displayed code in the **Word Verification** field as seen in the code display box. The code is not case sensitive and includes upper and lower case characters.
11. Optionally, review the Google Terms of Service.
12. Click the 'I accept. Create my account' button. Presented is a page similar to that depicted in Figure 8 and you have completed the registration process for your free Gmail account.

Figure 8: Introduction to Gmail page



**Appendix C: How to Create a Microsoft Hotmail Email Account**

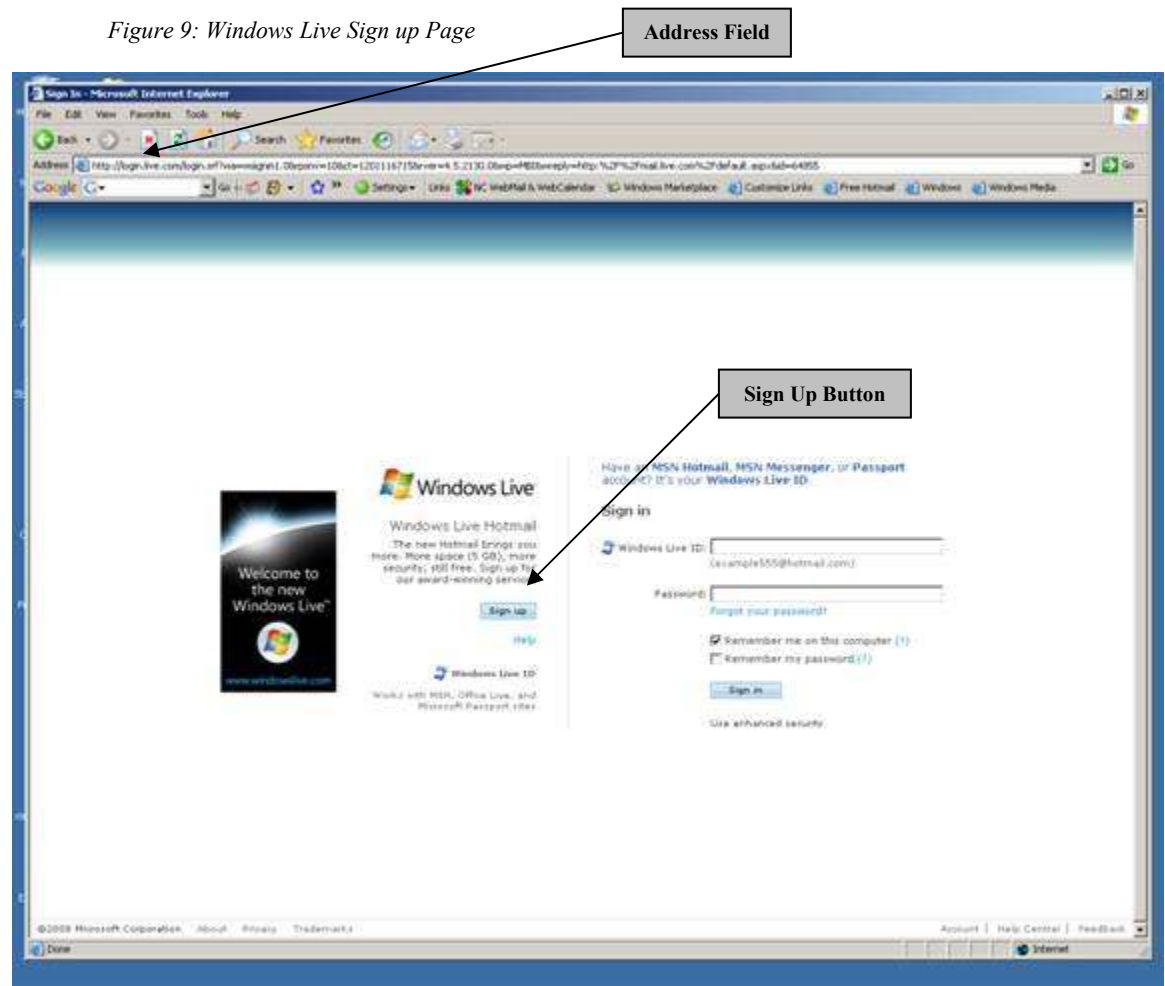
Hotmail is an online email service by Microsoft, and it gives the user up to 6 GB of storage as of January 2008. Here is how to create your free Hotmail account:

1. Open your preferred web browser (e.g., Internet Explorer, Netscape Navigator, Mozilla Firefox, and Apple Safari).

The home page for your web browser will appear.

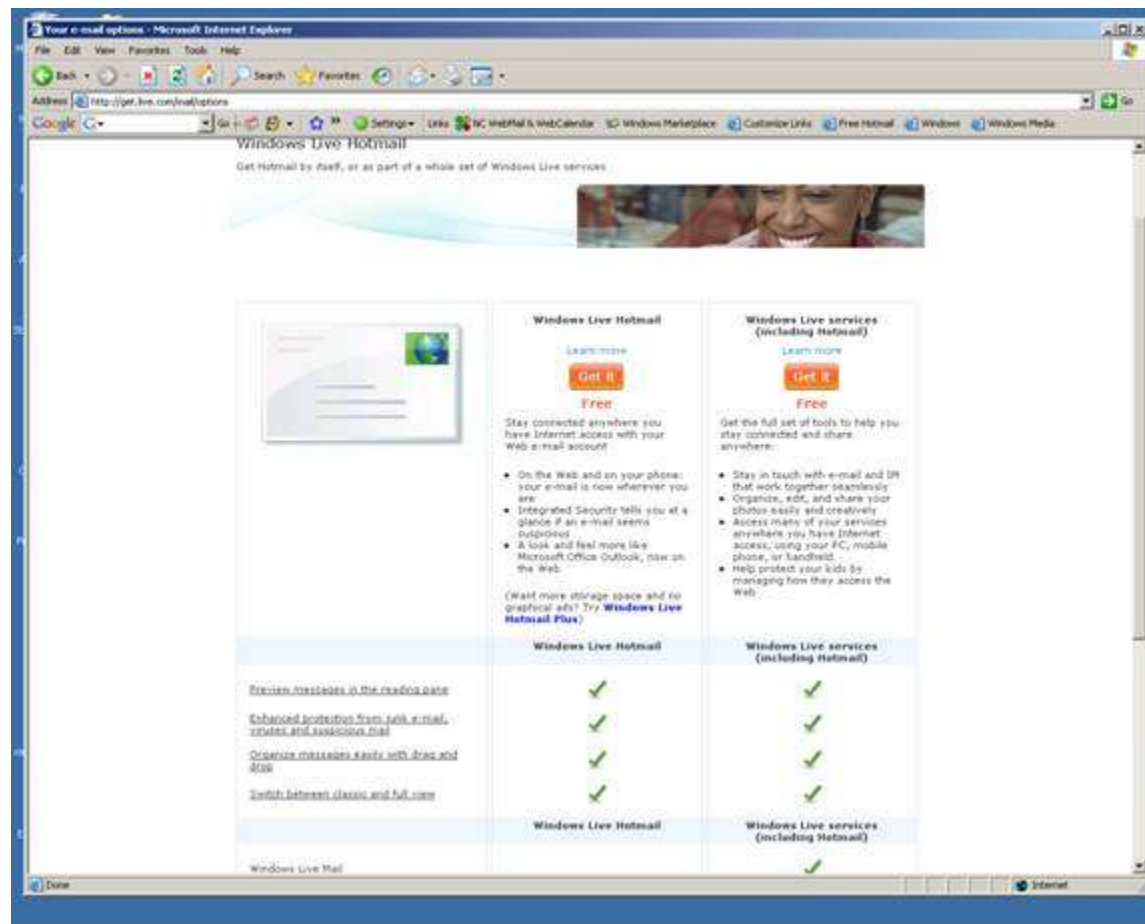
2. In the **Address** field, type <http://hotmail.com> and press the Enter or Return key on your keyboard. This will take you to the Windows Live signup page. Move your mouse cursor to and click on the blue Sign up button on the left, center side of the web page as depicted in Figure 9.

Figure 9: Windows Live Sign up Page



This takes you to the 'Get Windows Live Hotmail' window as depicted in Figure 10.

Figure 10: Get Windows Live Hotmail Page



3. Choose the orange 'Get it' button for Windows Live Hotmail. Please do not choose Windows Live services, as the instructions below cover its registration process.

This brings you to the 'Sign up for Windows Live' window, as shown below.

Figure 11: Sign up for Windows Live Page

4. There are several mandatory fields to complete. Enter the desired Windows Live ID in the **Windows Live ID** field. Once entered, click the 'Check availability' button to determine the availability of the desired ID. If unavailable, enter a different name and repeat the process. This will be your unique Hotmail email address.

Examples of a Windows Live ID name are:

- John.smith
  - Jane\_Doe
  - John1234
5. After selecting a valid desired login name, enter the desired password in the **\*Type password** field. The password should be at least six characters in length, using both letters and numbers. Re-enter the desired password in the **\*Retype password** field.
  6. Proceed to the Enter password reset information section. The **Alternate email** field is available, if desired; however, it is not a mandatory field.

7. Select a question from the drop down menu next to **\*Question**. Once selected, provide an answer to the question in the **\*Secret Answer** field.
8. Proceed to the Your Information section, and enter your first name and last name in the appropriate fields.
9. Select the appropriate gender.
10. Enter your birth year (e.g., 1999).
11. Keep the default setting for the **Country/Region** field set to United States.
12. Select North Carolina in the **State** field.
13. In the **Zip Code** field, enter the five-digit zip code for your work area.
14. Enter in the **Type characters** field the characters displayed in the picture box. Depicted in Figure 12 is an example of characters in the picture box.

Figure 12: Characters Picture Box

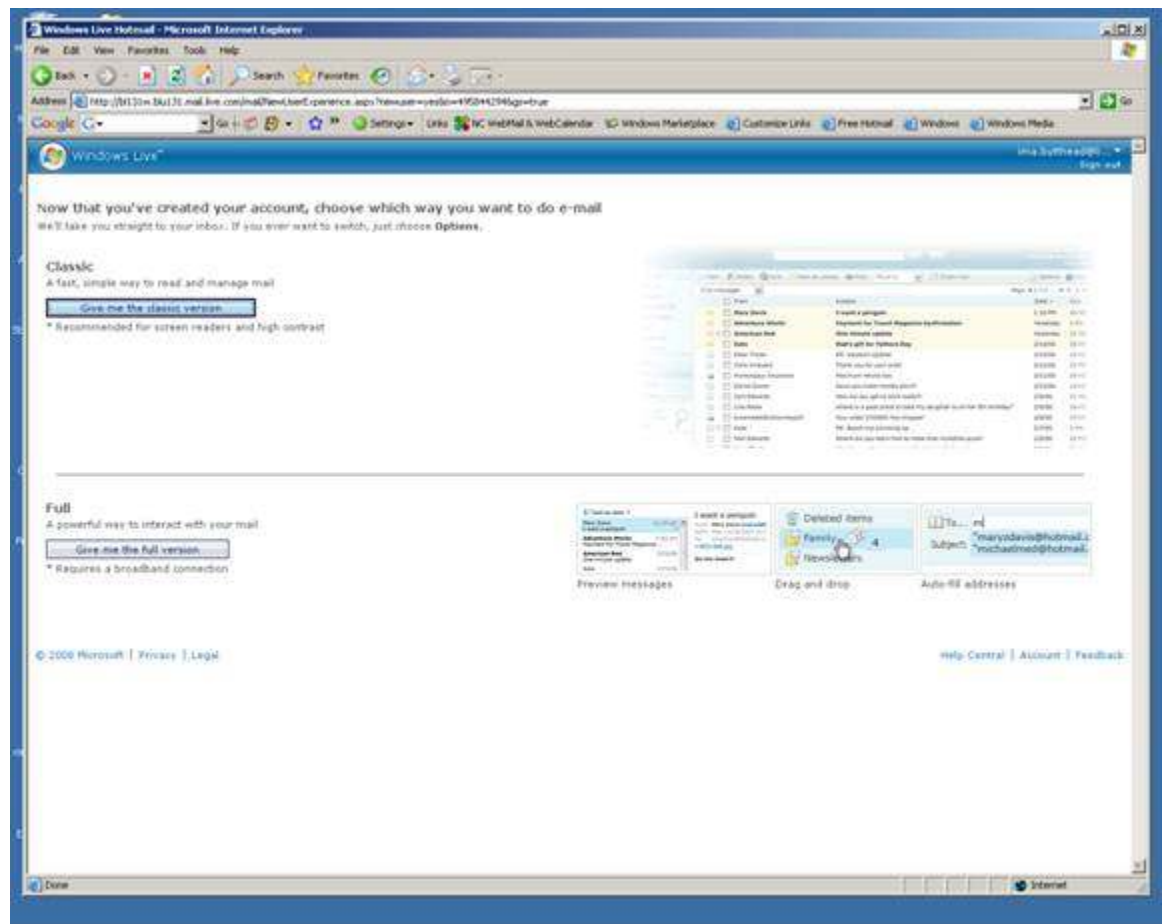
Type the characters you see in this picture

Picture: 

\*Type characters:

15. Optionally, review the Windows Live Service Agreement.
16. Click on the 'I accept' button. Presented is a page similar to that depicted in Figure 13 below.
17. Select either the Classic or the Full version of Hotmail, as desired. You have completed the registration process for your free Hotmail email account.

Figure 13: Microsoft Hotmail Account Creation Page





**Appendix D: How to Create a AOL Mail Email Account**

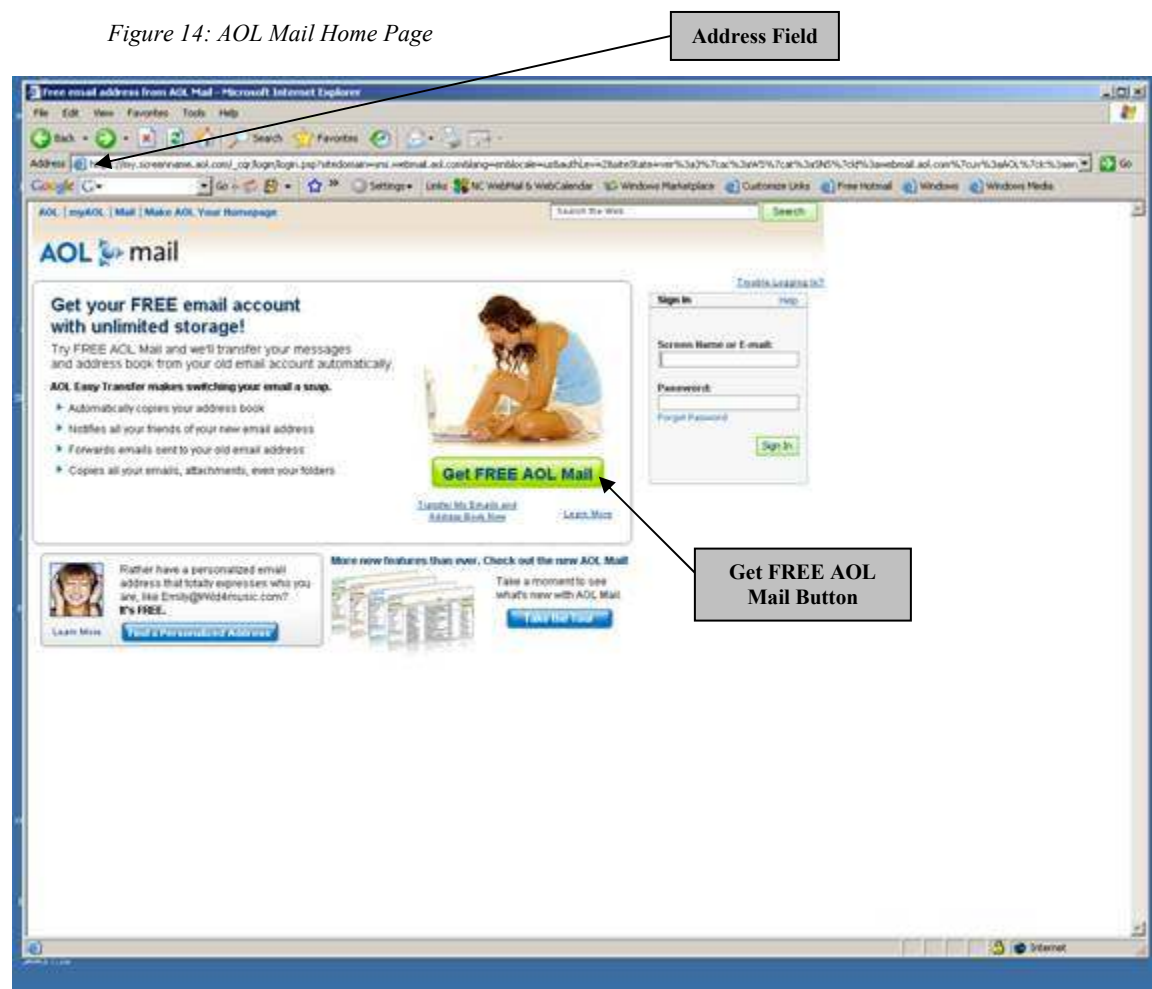
AOL Mail is an online email service by AOL and its main attraction is unlimited storage space for email. Here is how to create your free AOL Mail account:

1. Open your preferred web browser (e.g., Internet Explorer, Netscape Navigator, Mozilla Firefox, and Apple Safari).

The home page for your web browser will appear.

2. In the **Address** field, type `http://mail.aol.com` and press the Enter or Return key on your keyboard. This will take you to the AOL Mail signup page.
3. Click the green button that reads 'Get FREE AOL Mail'.

Figure 14: AOL Mail Home Page



This takes you to the 'Create an Account' window as depicted in Figure 15.

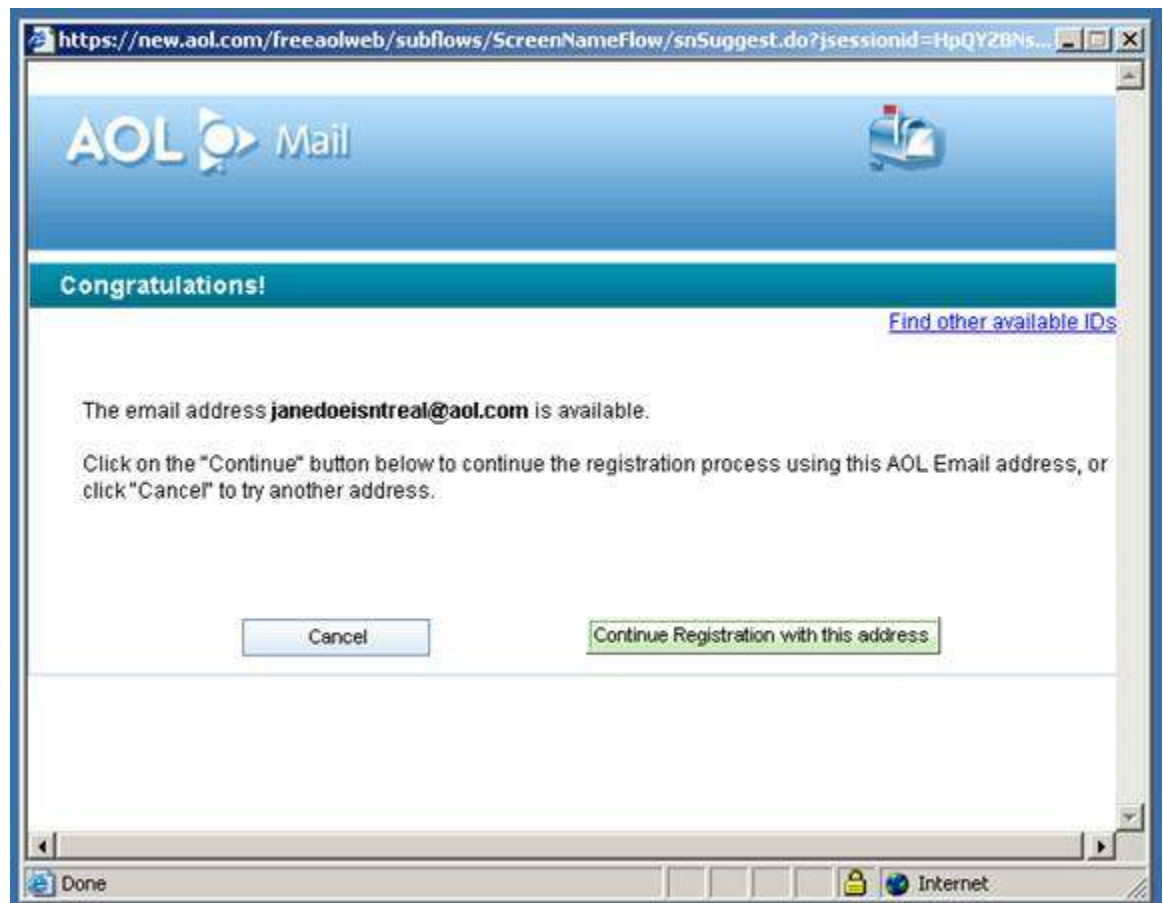
Figure 15: AOL Mail Create an Account Page

There are several mandatory fields in the window you will now fill including First Name, Last Name and Desired Login Name.

4. Enter your First Name and Last Name in the appropriate fields.
5. Enter in the desired Email Address in the **Desired Email Address** field.

Examples of an Email address name are:

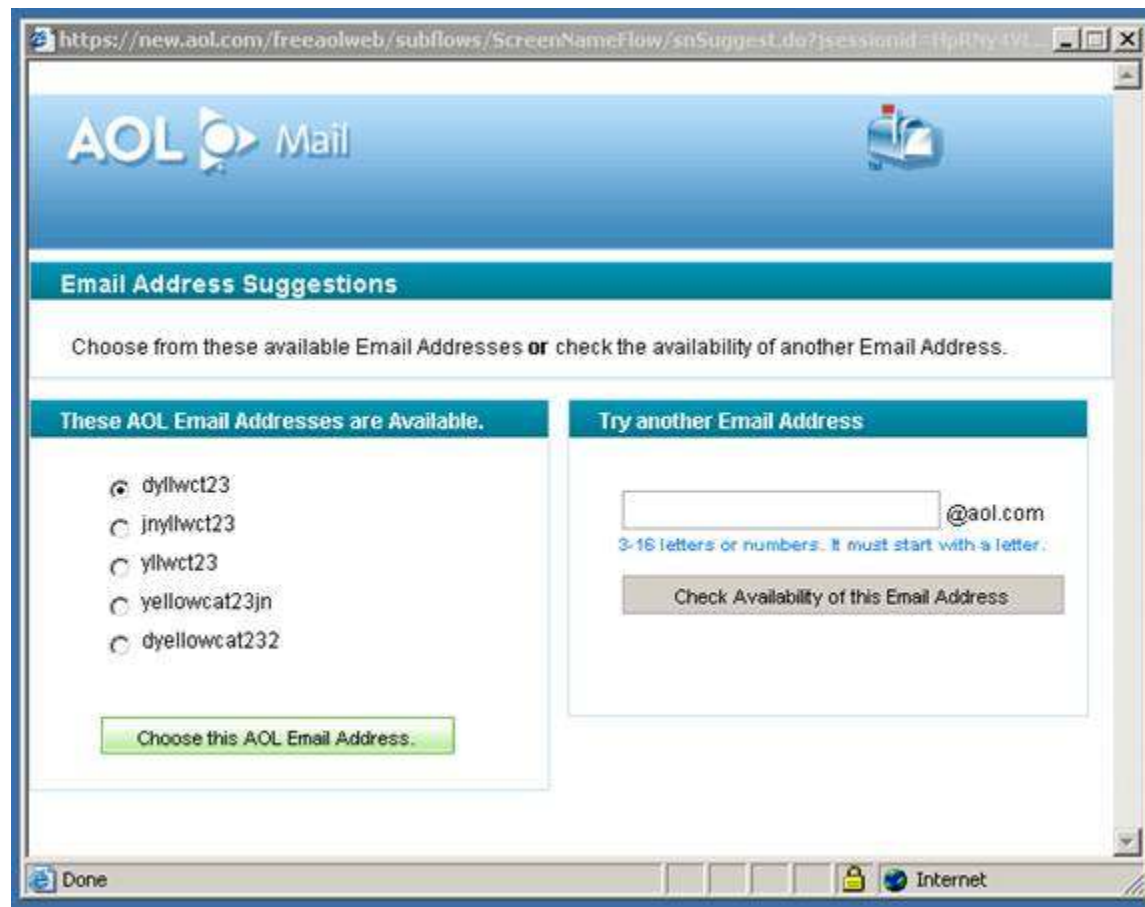
- John.smith
  - Jane\_Doe
  - John1234
6. Once entered, click the grey 'Check Availability of this Email Address' button. If your desired name is available, the process will bring up a secondary screen similar to that depicted in Figure 16.

*Figure 16: AOL Email Address Congratulations Page*

7. Click on the green 'Continue Registration with this address' button.

If your desired email address is not available you will receive a secondary window similar to the following:

Figure 17: AOL Email Address Suggestions Page



8. Select one of the suggested Email addresses on the left or continue to try another on the right.
9. After selecting an available Email address, click the green 'Choose this AOL Email Address' button.

This will take you back to the primary screen where you will continue the registration by creating your password.

10. Enter the desired password in the **Password** field. The password must be between six and sixteen characters in length, using both letters and numbers. Re-enter the password in the **Re-type password** field.
11. Under the 'Tell Us About Yourself' section, you are required to fill in the fields for:
  - Street Address
  - City

- State
- Zip Code
- Phone
- Birthday
- Gender

Enter the appropriate information as requested in these mandatory fields. If desired, you may use your work address and phone number, rather than your home address and phone number.

12. Select a security question using the drop down menu under **Account Security Question**. Once selected, provide the answer in the **Your Answer** field. Retype the answer in the **Re-type Answer** field.
13. In the 'Verify Your Registration' section, enter the characters displayed in the picture in the grey box.
14. Optionally, review the AOL Terms of Service.
15. Click on the green 'Submit' button. Presented is a window with confirmation for creating your new AOL Mail account.

## Appendix E: Acceptable Use for DHHS Information Systems

***Note.** The following policy is copied from the DHHS Online Publications, Department-Wide Publications web site. Employees are responsible for ensuring conformance to the latest policy, which is available online via [http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/12acceptable\\_use.pdf](http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/12acceptable_use.pdf).*

### DHHS POLICIES AND PROCEDURES

Section VIII:	Security and Privacy
Title:	Security Manual
Chapter:	Acceptable Use for DHHS Information Systems
Current Effective Date:	6/15/05
Revision History:	This policy replaces DHHS Policies and Procedures, Computer Use Policy, Section III: Communications, dated 4/01/04.
Original Effective Date:	8/1/04

### Purpose

This policy defines the information system security responsibilities and acceptable use rights for employees, volunteers, guests, vendors and contractors (hereinafter, “**Users**”) of North Carolina Department of Health and Human Services (“**DHHS**”, or alternatively, the “**Department**”) information system resources.

Information systems include all platforms (operating systems), all computer sizes (personal digital assistants through mainframes), and equipment, and all applications and data (whether developed in-house or acquired from third parties) contained on those systems.

This policy document includes an agreement form that once signed, certifies the User’s understanding and affirmation of the policy.

### Policy

Each DHHS Division/Office shall be responsible for ensuring that every individual seeking access to DHHS network and/or information systems reviews this policy and signs an acceptable use agreement based upon the terms specified in this policy. Users must sign the agreement form included herein before permission is granted to use the DHHS systems.

### Implementation

#### 1. User Access Responsibilities

All information and data processing systems to which users are given access are to be used only to conduct the activities authorized by the Department. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the Department or on its behalf. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of Department, State, and/or Federal laws which will result in disciplinary action consistent with the policies and procedures of the Department (see **Enforcement** section below).

DHHS Divisions/Offices may require additional agreements regarding the confidentiality of specific types of information; for example, medical records, client case files, personnel records,

financial records, etc. This policy may augment such Division/Office policies, but is not intended to replace such policies, which remain in effect.

## **2. Rights of Information Ownership**

The Department and its Divisions/Offices retain the rights of ownership to all IS resources including hardware, software, functionality, data, and related documentation developed by the Department's information systems users on behalf of the Department. All Department IS resources remain the exclusive property of the State of North Carolina and/or the Department, unless otherwise prescribed by other contractual agreements.

## **3. Use of NC Integrated Information Network ("NCIIN") and the Internet**

The Internet is a world-wide collection of interconnected computer networks. The State's wide area network, NCIIN, is the NC controlled network connected to the Internet.

Following is a list of policies regarding the use of NCIIN and the Internet:

1. While in performance of work-related functions, while on the job, or while using publicly owned or provided information processing resources, DHHS users are expected to use the NCIIN and Internet responsibly and professionally. Users shall make no intentional use of these services in an illegal, malicious, or obscene manner as described in NC General Statute (GS) 14-190.1. Users may make reasonable personal use of publicly owned or provided NCIIN or Internet resources as long as:
  1. The direct measurable cost to the public is none, is negligible, or access supports the mission of the agency;
  2. There is no negative impact on user's performance of public duties;
  3. The policy is applied equitably among all personnel of the agency;
  4. Users may be required to reimburse the agency if costs are incurred that do not have prior approval by the Agency or Division/Office.
2. When sending or forwarding e-mail over the NCIIN or the Internet, Users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law to make anonymous postings.
3. Users are responsible for protecting DHHS sensitive information by following the DHHS policies and DHHS Division/Office policies and procedures.
4. Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via NCIIN and the Internet is accurate. Users shall provide in association with such information the date at which it was current and an e-mail address allowing the recipient to contact the public staff responsible for making the information available in its current form.
5. Users shall avoid unnecessary network traffic and interference with other users, including but not limited to:

1. Unsolicited commercial advertising by DHHS Users. Such use is strictly forbidden. For the purpose of this Policy, “unsolicited commercial advertising” includes any transmission that describes goods, products, or services and that is initiated by a vendor, provider, retailer, or manufacturer of the described goods, products or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer. For purposes of this definition the vendor, provider, retailer, or manufacturer must be a non-governmental entity. This prohibition shall not include:
  1. Discussions of a product or service’s relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer or manufacturer, or related or affiliated with the vendor, provider, retailer, or manufacturer),
  2. Responses to questions, but only if such responses are direct replies to those who inquired via e-mail, or
  3. Mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.
2. The use of computer resources, including e-mail, to conduct any activities already prohibited by the Office of State Personnel or other DHHS policies (such as private/personal fund raising, political activities, etc.) shall be prohibited.
3. Mass emailing by public employees and NCIIN users that do not pertain to governmental business is prohibited.
4. Users shall not use the Internet, the NCIIN, or any State information system to (i) allow the unauthorized dissemination of confidential information, or (ii) for any purpose that is not permitted by DHHS policies or would compromise public safety or public health.
5. Users shall not stalk others; post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, a civil liability, or violation of any applicable law.
6. Users shall not access or attempt to gain access to any computer account to which they are not authorized. They shall not access or attempt to access any portions of the NCIIN networks to which they are not authorized. Users also shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.
7. Users given access to which they are not privileged or entitled, are required to report the circumstances immediately to their supervisor. Supervisors are responsible for determining the User’s appropriate access rights. Supervisors must notify their Division/Office Information Security Official should they determine that access rights need to be modified.



#### 4. Workstation Security

These requirements apply to office, home or other remote access locations if utilized for DHHS business.

1. As appropriate, sensitive paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, or behind locked doors, especially outside working hours.
2. Personal computers and computer terminals should not be left logged on when unattended or not in use. Personal computers or computer terminals shall be protected from unauthorized access by physical, technical, or administrative controls such as passwords, time driven screensavers, controlled workstation access, operational procedures, etc.
3. Classified or sensitive information should not be printed on a printer located in public areas. However, in the event that public printers must be used to print sensitive or classified information, such information shall be cleared from printers immediately.
4. Users shall adhere to the requirements of [ITS Desktop and Laptop Security Standard](#).

#### 5. Media Storage

1. Classified information stored on external media (e.g., diskettes or CDs) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as classified information.
2. The use of removable storage devices or external devices (e.g., USB Flash Drives) shall be restricted to authorized personnel in order to safeguard and protect confidential data and information technology assets. Authorization for the use of removable storage devices must be granted by the user's supervisor in writing and specify the intended use of the device. The Division/Office security official shall maintain an inventory of all authorizations and use of removable storage devices. Any use must meet DHHS security policies and standards.

Users shall request the use of state owned storage devices. Division/Offices shall strive to provide state owned-storage devices to staff and there by limit the use of any personal device used to conduct any state business. Any use of personal devices must be disclosed to the supervisor and be approved.

3. Mobile computing devices and removable storage devices (e.g., laptops, PDAs, USB flash drives, etc) must never be left in unsecured areas and their use must meet DHHS Security Standards. Any incidents of misuse, theft or loss of data must be reported to the supervisor and to the Division Security Official. The incident should be reviewed and reported in accordance with the DHHS Incident Management Policy.
4. DHHS sensitive or confidential information shall not be stored at home without appropriate authorization from the user's supervisor/manager, in consultation with the Division/Office Security Official. Users shall follow appropriate physical safeguards for offsite use. Documentation of authorization and storage of sensitive information in the home shall be maintained in accordance with the Division/Office's procedures.

## **6. User Privacy**

All users of the Department's information systems are advised that their use of these systems may be subject to monitoring and filtering. DHHS reserves the right to monitor – randomly and/or systematically – the use of Internet and DHHS information systems connections and traffic. Any activity conducted using the State's information systems (including but not limited to computers, networks, e-mail, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable Departmental policies and State and Federal laws or rules. The Department reserves the right to perform these actions with or without specific notice to the user.

## **7. Software License Agreements**

1. The theft of computer resources, including computer software, is illegal. All computer software, including software obtained from sources outside the Department, is subject to license agreements that may restrict the User's right to copy and use the software. Software distributed on a trial basis, even through the Internet, does not suggest that the software is free or that it may be distributed freely.
2. The Department does not require, request, or condone unauthorized use of computer software by its employees, volunteers, and contractors. The Department enforces Federal Public Law 102-561, which strictly prohibits any violation of copyright protection. Violation of copyright protection is considered a felony and is punishable by up to five years in prison and/or fines up to \$250,000 for all parties involved.

## **8. Computer Viruses: Malicious Code**

1. It is the responsibility of each User to help prevent the introduction and spread of computer viruses and other malicious code. All personal computers in the Department must have virus detection software running at all times. All files received from any unknown source external to the Department, including those on storage on media and electronically downloaded or received as e-mail attachments, except for attachments received via NCMail, must be scanned for computer viruses before opening or using the files. (Attachments received via NCMail are automatically scanned.)
2. Users should immediately contact their manager or supervisor, other appropriate designated staff or the Division/Office Security Official when a virus is suspected or detected, so that it may be confirmed and removed by the appropriate staff.
3. Users must report all information security violations to the Division/Office Security Official, who will notify the DHHS Privacy and Security Office in accordance with the Incident Management policy and procedures. The DHHS Security Officer shall be responsible for notification of the ITS Security Office.

## **9. Installation of Hardware or Software**

1. DHHS information system hardware and software installations and alterations are handled by authorized DHHS employees or contractors only. Users shall not install new or make changes to existing information system hardware or software.

2. Users shall not download software from the Internet unless specifically approved by the user's supervisor and the designated IT personnel. Downloading audio or video stream for a work-related webinar or audio conference is permissible without prior authorization.

#### 10. Remote Access

1. Authorized users of DHHS's computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks and data repositories to conduct state-related business only. Users will only be granted remote access through secure, authenticated and managed access methods and in accordance with the ITS and DHHS Remote Access Security Policy and Standard.
2. Users shall not access agency networks via external connections from local or remote locations, including homes, hotel rooms, wireless devices, and off-site offices without knowledge of and compliance with the User Access Responsibilities section described above within this policy.

### Enforcement

*For enforcement questions or clarification on any of the information contained in this policy, please contact [DHHS Security Officer](#). For general questions about department-wide policies and procedures, contact the [Office of Policy & Planning](#).*

### Exceptions

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [ITS Waiver and Appeals Policy](#).

#### USER CERTIFICATION OF NOTIFICATION AND AGREEMENT OF COMPUTER USE POLICY

I certify that I am an employee, volunteer, guest, vendor or contractor working for or on behalf of the Department of Health and Human Services and that I have read this "Acceptable Use Policy" and understand my obligations as described herein. I understand that this policy was approved by the Secretary of the Department of Health and Human Services and these obligations are not specific to any individual Division or Office of the Department, but are applicable to all employees, volunteers, and contractors of the Department. I understand that failure to observe and abide by these obligations may result in disciplinary action, which may include dismissal and/or contract termination. I also understand that in some cases, failure to observe and abide by these obligations may result in criminal or other legal actions. Furthermore, I have been informed that the Department will retain this signed Agreement on file for future reference. A copy of this Agreement shall be maintained in the personnel file and/or in the contract administration file.

Print Name _____	
Employee, Volunteer, Guest, Vendor or Contractor Signature _____	Date _____
Supervisor's Signature _____	Date _____

\*\*\*End of Document\*\*\*